WHERE THE WILD THINGS ARE:

ENCRYPTION, POLICE ACCESS, AND THE USER

BY WHITNEY MERRILL (@WBM312)

A B O U T M E

Whitney Merrill (@wbm312)

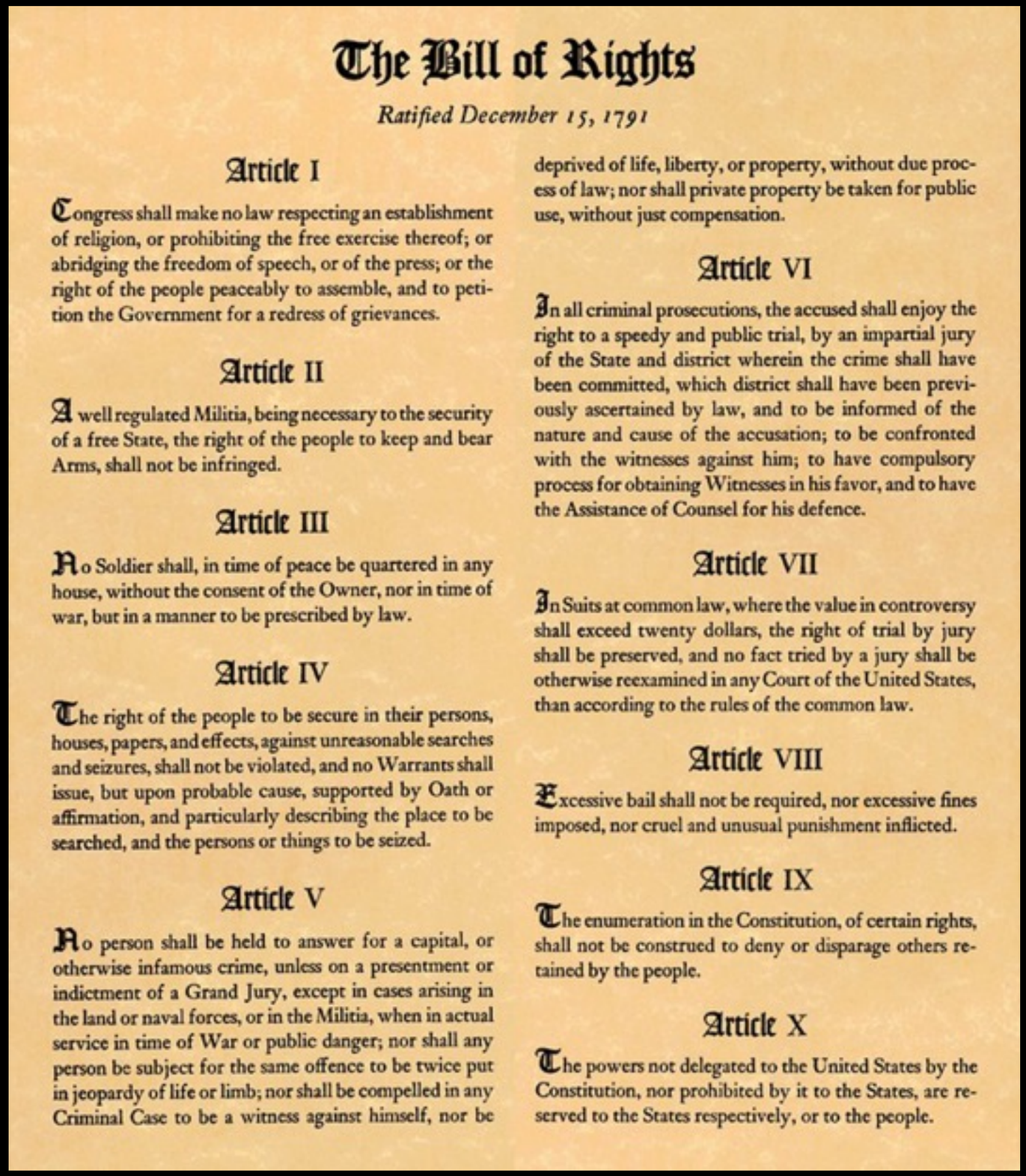
- Lawyer
- Master’s student in Computer Science with a focus in information security @ the University of Illinois Urbana-Champaign
- Research: privacy, usability of encryption, legal and policy issues surrounding technology and information security

OBLIGATORY DISCLAIMER:

- I am not your lawyer.
- This presentation is not legal advice.
- With that being said…

WHAT I PLAN TO COVER

- The Issues & Background
  - 1st Amendment
  - 4th Amendment
    - Probable cause & encryption
  - 5th Amendment
    - Self-incrimination
  - All Writs Act
- Research on use of encryption
- Backdoor access
- Going Forward
- Questions (hopefully)



The Bill of Rights

Ratified December 15, 1791

Article I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Article II

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

Article III

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Article IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any Criminal Case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Article VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining Witnesses in his favor, and to have the Assistance of Counsel for his defence.

Article VII

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury shall be otherwise reexamined in any Court of the United States, than according to the rules of the common law.

Article VIII

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishment inflicted.

Article IX

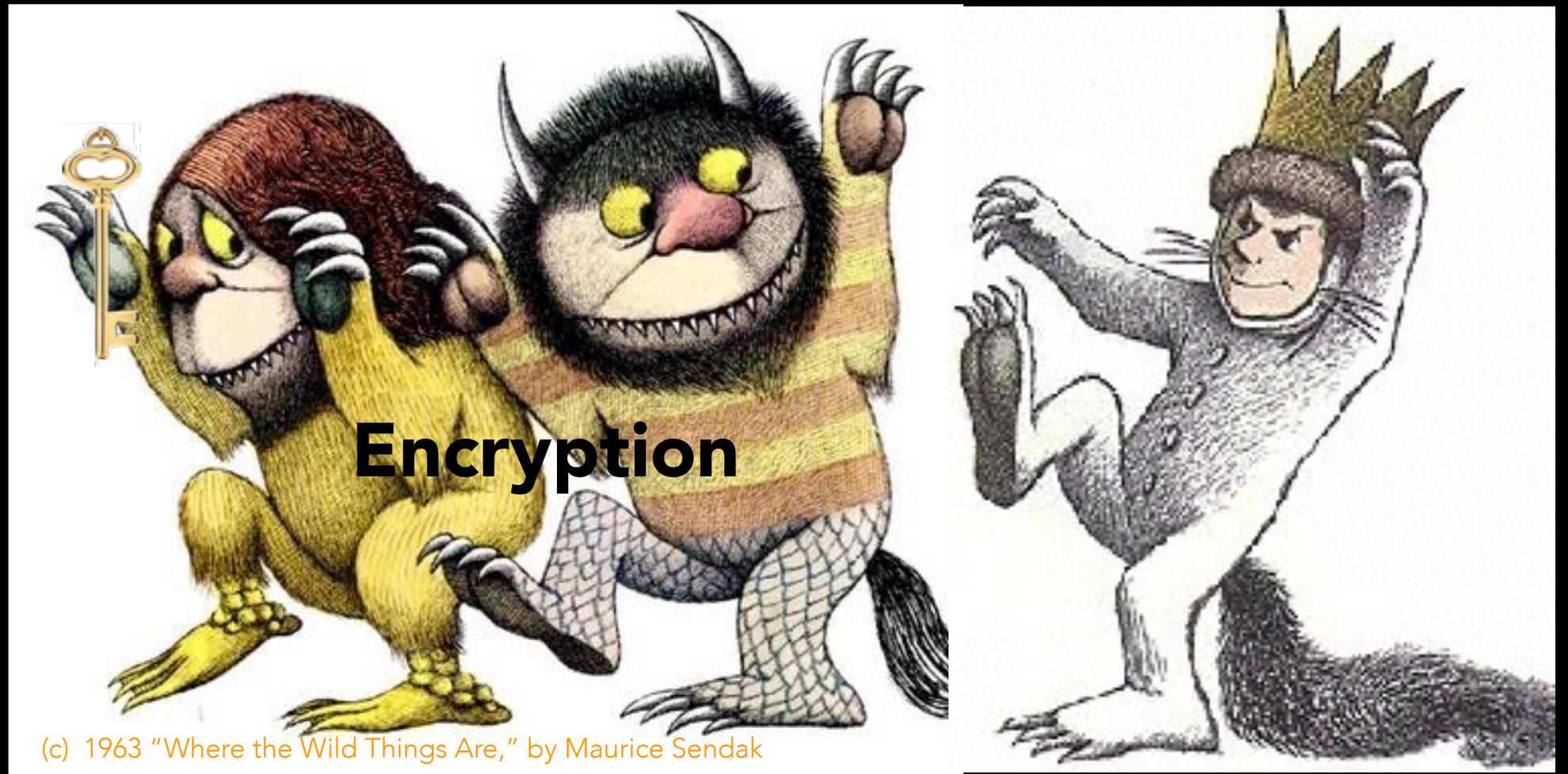
The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Article X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

THEME

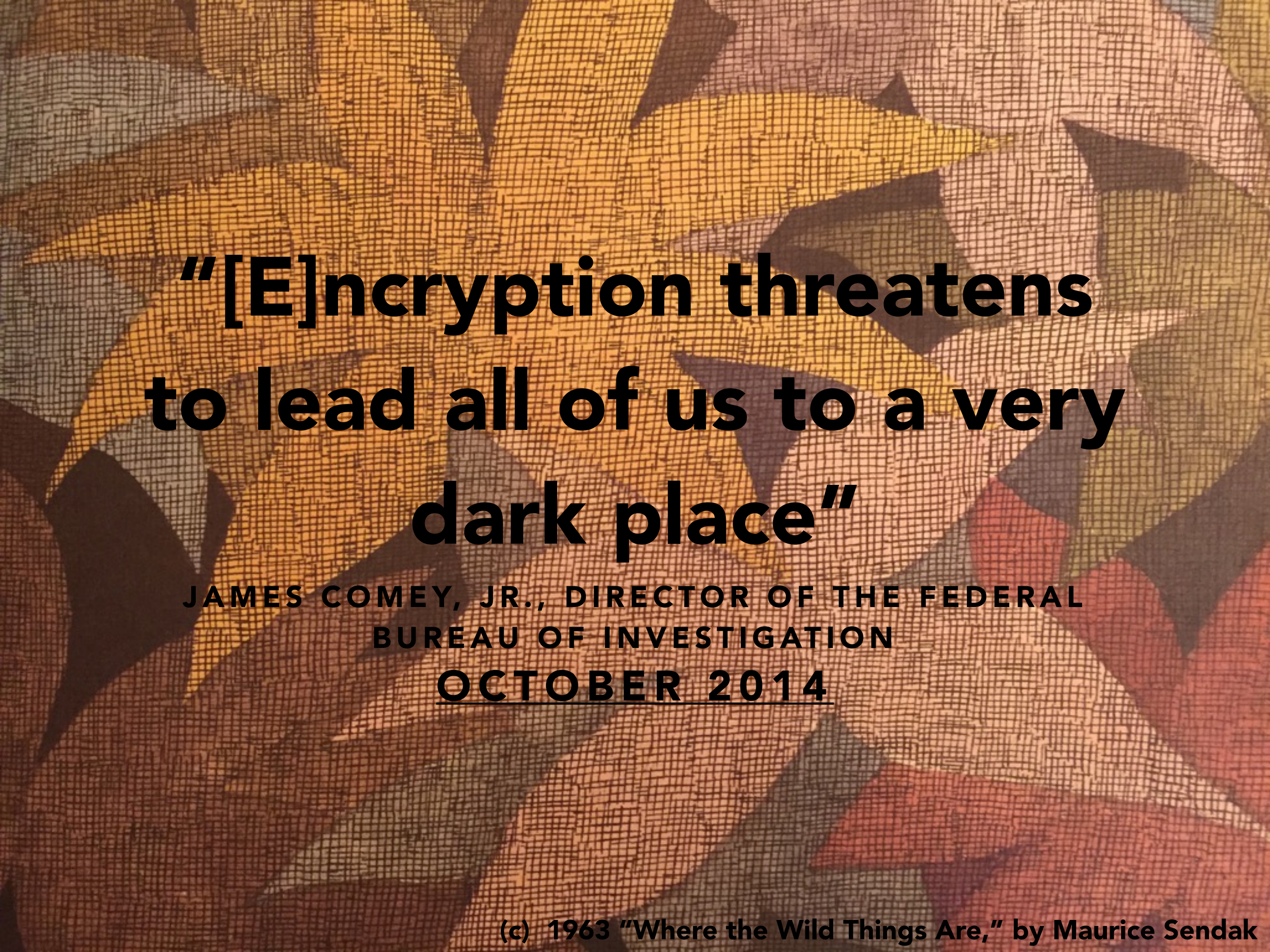
- Why “[e]ncryption is an altogether different beast” under the law, and why that scares the government.



(c) 1963 “Where the Wild Things Are,” by Maurice Sendak

"In several major hacker cases, the subjects have encrypted computer files, thereby concealing evidence of serious crimes. In one such case, the government was unable to determine the full scope of the hacker's activity because of the use of encryption."

PREPARED STATEMENT OF ROBERT S. LITT,
DEPUTY ASSISTANT ATTORNEY GENERAL,
CRIMINAL DIVISION, DEPARTMENT OF JUSTICE
SECURITY AND FREEDOM THROUGH ENCRYPTION
(SAFE) ACT
MARCH 20, 1997 - HOUSE JUDICIARY SUBCOMMITTEE
ON COURTS AND INTELLECTUAL PROPERTY


"[E]ncryption threatens to lead all of us to a very dark place"
JAMES COMEY, JR., DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
OCTOBER 2014
(c) 1963 "Where the Wild Things Are," by Maurice Sendak

Governments fear encryption will allow the "Four Horsemen of the Infocalypse (**software pirates, organised crime, child pornographers, and terrorists**)" to thwart prosecution.

TERM "INFOCALYPSE": CORY DOCTOROW, "CRYPTO WARS REDUX: WHY THE FBI'S DESIRE TO UNLOCK YOUR PRIVATE LIFE MUST BE RESISTED"

SOMETHING TO THINK ABOUT...

As encryption becomes more user friendly and more widely implemented, how will the government seek to weaken it or control its implementation?

Under the law, **could** they and **should** they be successful in doing so?

"The new issue may be a Fifth Amendment question rather than a Fourth Amendment debate. '**Encryption is an altogether different beast.** In most cases involving encryption, police already possess the device containing the encrypted data; the problem is that they cannot read the data.' **'[F]orcing an arrestee to reveal an encryption key may impinge on a defendant's right against self-incrimination**. In contrast to the Fourth Amendment warrant exception, 'the privilege against self-incrimination has **no warrant exception**.'

UNITED STATES V. LUSTIG, 13CR3921-BEN, 2014 WL 940502 (S.D. CAL. MAR. 11, 2014)(JUDGE ROGER T. BENITEZ QUOTING HON. BRIAN M. HOFFSTADT)

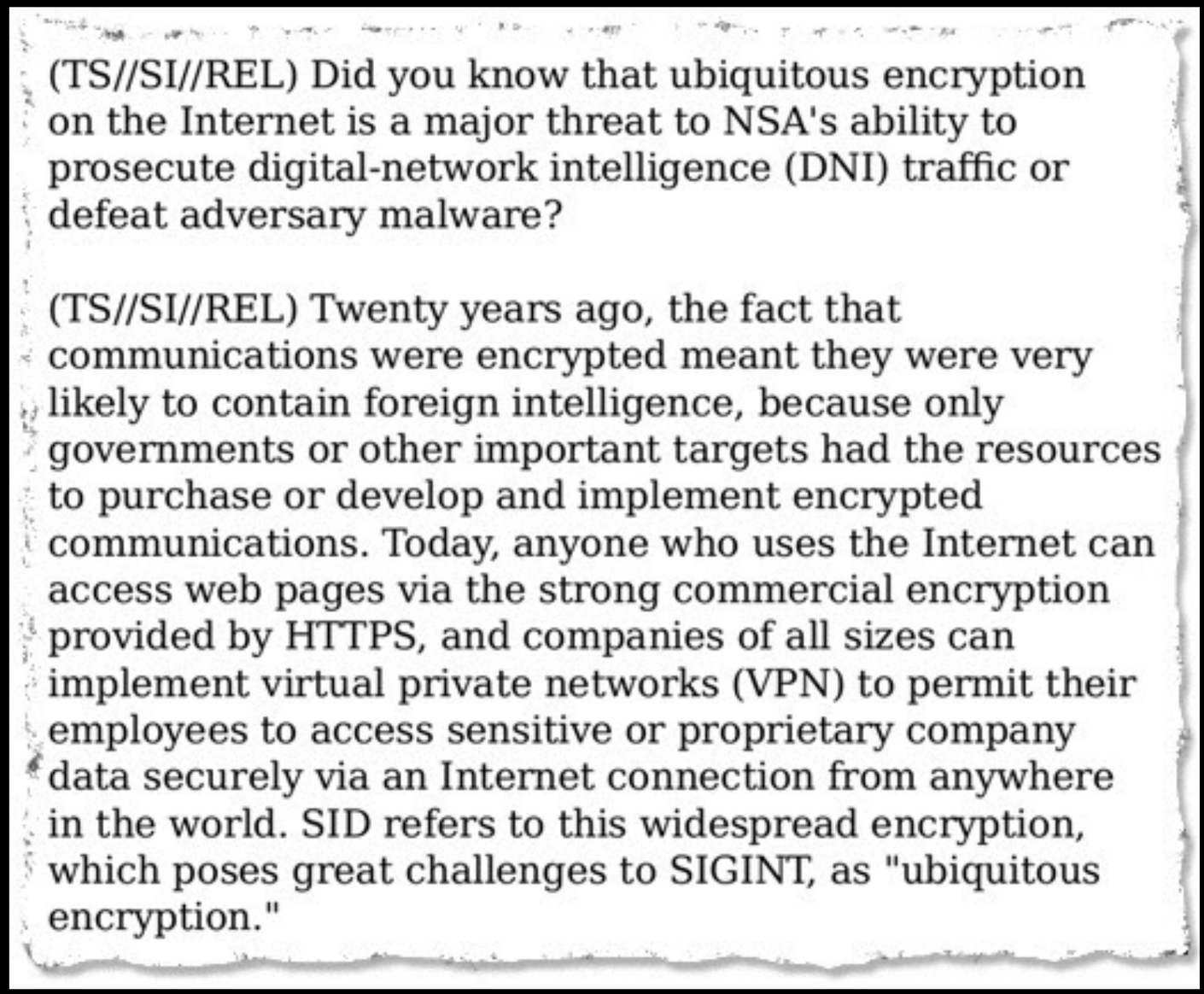
"In other words, future cell phones may automatically encrypt user data. If police cannot decipher the contents of the phone, whether saved in a Faraday bag or not, **the only solution may be to gain the encryption key from the arrestee**. To do that, prosecutors could be forced to grant the arrestee **immunity**. '[T]he privilege against self-incrimination could well put encrypted data forever beyond the reach of law enforcement.'"

UNITED STATES V. LUSTIG, 13CR3921-BEN, 2014 WL 940502 (S.D. CAL. MAR. 11, 2014)(JUDGE ROGER T. BENITEZ QUOTING HON. BRIAN M. HOFFSTADT)

USABILITY

HISTORY

- Encryption used by few
- Tools not built in
- Not available on all devices
- Tools were flawed, hard to use, or implement
  - Ahem…Cough…PGP



(TS//SI//REL) Did you know that ubiquitous encryption on the Internet is a major threat to NSA's ability to prosecute digital-network intelligence (DNI) traffic or defeat adversary malware?

(TS//SI//REL) Twenty years ago, the fact that communications were encrypted meant they were very likely to contain foreign intelligence, because only governments or other important targets had the resources to purchase or develop and implement encrypted communications. Today, anyone who uses the Internet can access web pages via the strong commercial encryption provided by HTTPS, and companies of all sizes can implement virtual private networks (VPN) to permit their employees to access sensitive or proprietary company data securely via an Internet connection from anywhere in the world. SID refers to this widespread encryption, which poses great challenges to SIGINT, as "ubiquitous encryption."

Source: Der Spiegel,
“Prying Eyes: Inside the NSA's War on Internet Security”

GIZMODO

+ FOLLOW

Google Follows Apple in Encrypting Phone Data by Default

Chris Mills
Filed to: GOOGLE 9/18/14 8:36pm

ars technica

MAIN MENU ▾ MY STORIES: 6 ▾ FORUMS SUBSCRIBE JOBS

INFINITE LOOP / THE APPLE ECOSYSTEM

Apple expands data encryption under iOS 8, making handover to cops moot

"Apple cannot bypass your passcode and therefore cannot access this data."

by **Cyrus Farivar** - Sept 17 2014, 11:57pm CDT

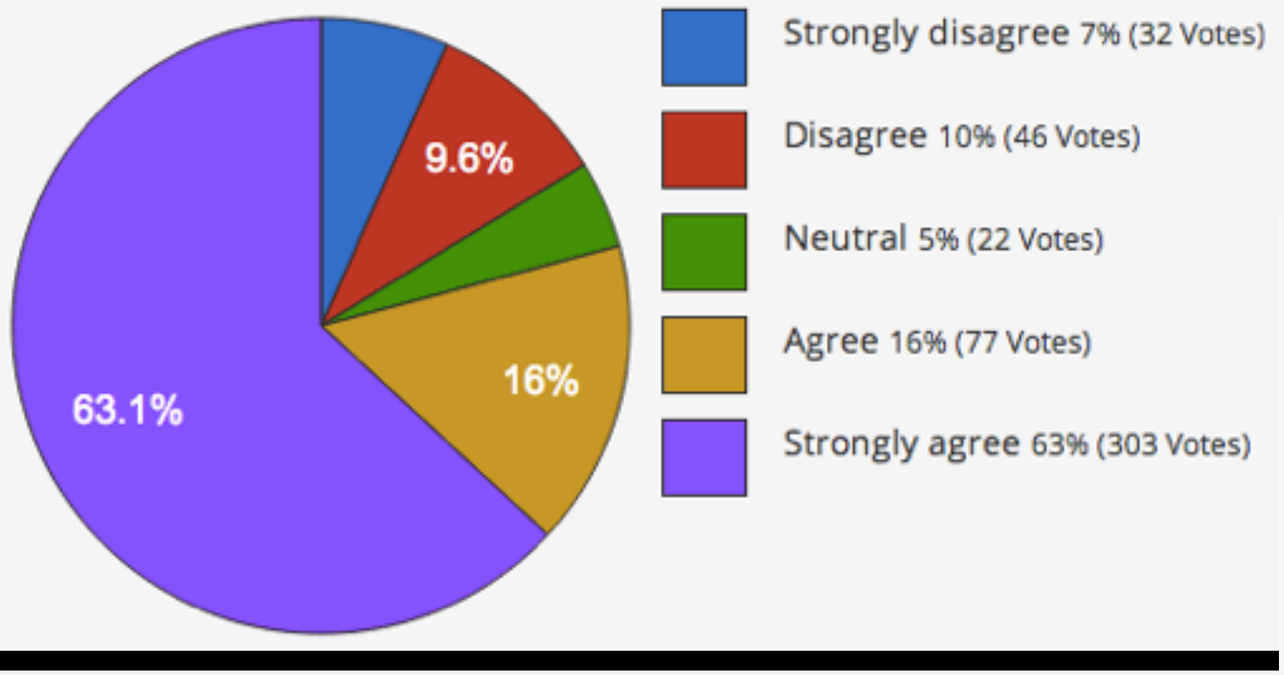
Share Tweet 335

Apple

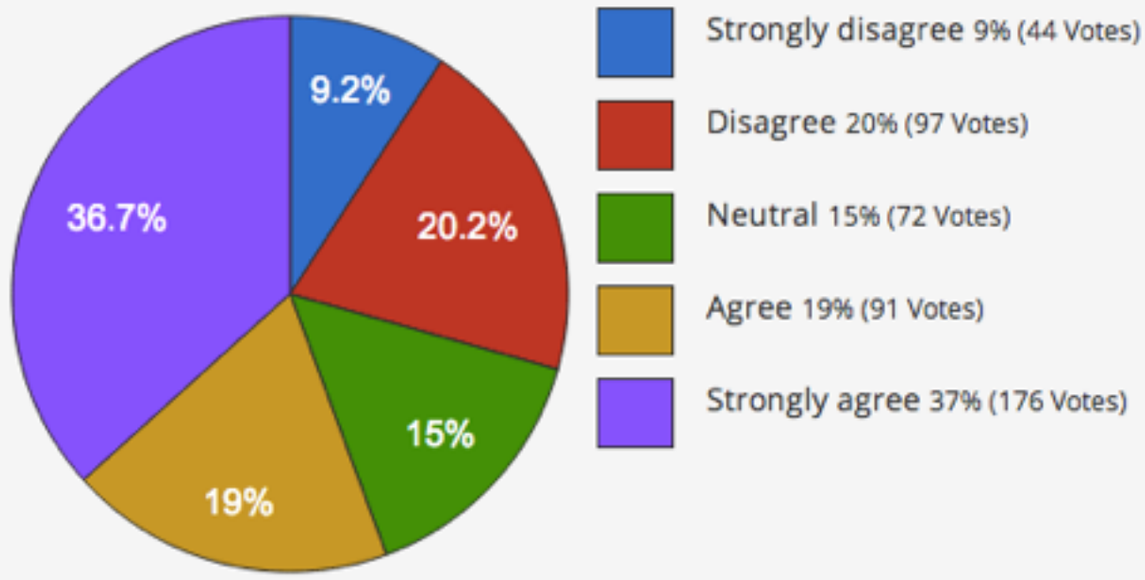
Apple defies FBI and offers encryption by default on new operating system

New version of Mac OS X will encrypt users' hard drives unless they explicitly decline, in spite of pleas by the FBI not to

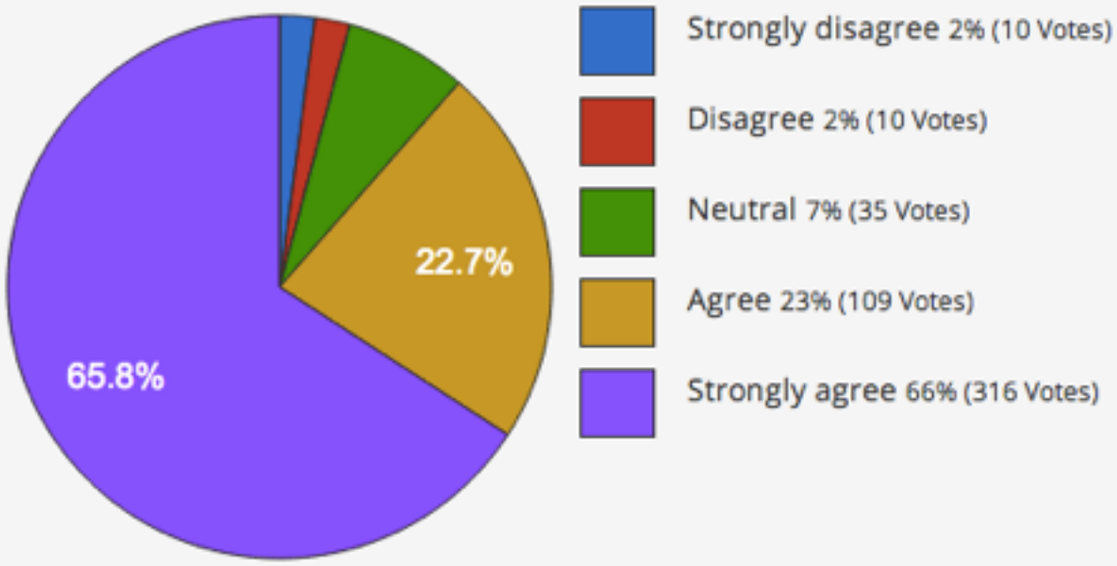
2- I always password protect my phone.



3- I use disk encryption on my computer.

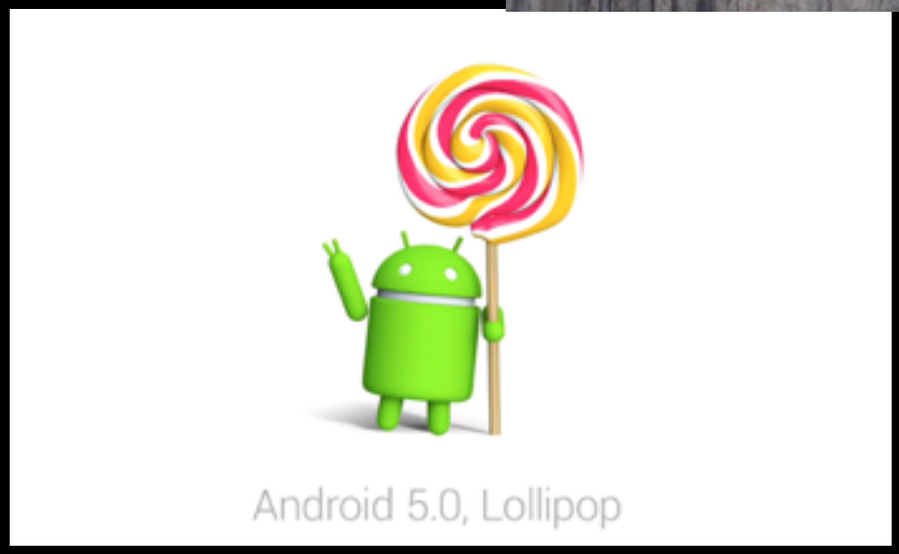


4- I would use encryption if it were easy to use and implement.



ENCRYPTION BY DEFAULT

- MacOS 10.10 Yosemite
- Linux (not by default but prompted to enable when installing Linux distribution of choice)
- Chrome OS
- iOS8
- Android 5.0 Lollipop



Written by
JASON KOE
STAFF WRITE

The Coming War Over

Intellectual Property Practice Gro
Issue 1, Spring 1998

By Eric Vance

Overview
Key Stories
Legislation
Key Players
Opinions
Links and Resources
Talk

Technology | CYBERTIMES
The New York Times ON THE WEB
Home Site Index Site Search Forums Archives Mar

January 28, 2000

CYBER LAW JOURNAL By CARL S. KAPLAN BIO

Wrinkle in Mitnick Case Hints at Encryption Battles to Come

A little-known legal skirmish in the case of the computer hacker Kevin Mitnick was a preview of similar fights to come as more people use encryption software to protect their files, lawyers who were involved in the case say.

Mitnick left federal prison last week after serving nearly five years for a series of crimes involving computer fraud and wire fraud. But his lawyers say they are still troubled by the judge's answer to a legal question raised early in the case: When federal agents seize encrypted files from a defendant, can they refuse to return them unless the defendant turns over the secret "key" to decode the files?

Deciphering Encryption

By Dan Froomkin
Washingtonpost.com Staff
and Amy Branson
LEGI-SLATE News Service
Updated May 8, 1998

The very same data-scrambling technology that can let you send your credit card number across the Internet without a qualm or e-mail a friend in absolute privacy may also make it harder for law enforcement authorities to detect terrorist plots or build cases against criminals.

Due to recent developments in software and hardware, some consumer-level encryption products are now so powerful that law enforcement officials say they can't crack them, even with massive supercomputers.

the hottest hi-tech issues on Capitol
her the government should step in and
products to maintain law
to eavesdrop electronically on anyone

ryption
ent

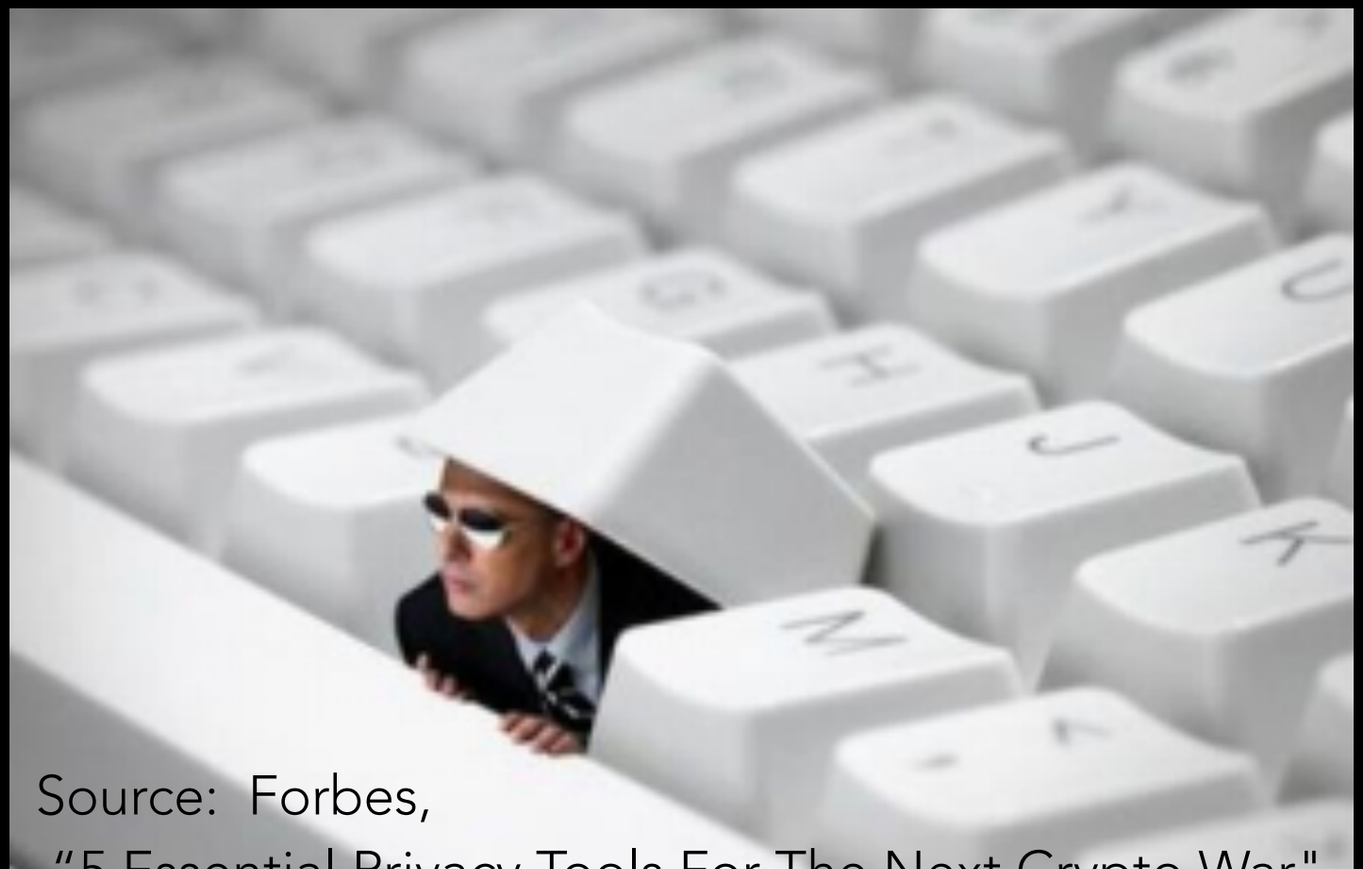
Top Stories
• U.S. to Relax Encryption Limits (Washington Post, Sept. 17)
• Harry and Louise Have a New Worry: Encryption (Washington Post, July 28)

1ST AMENDMENT

"Congress shall make no law . . . abridging the freedom of speech . . . ."

CRYPTO WARS

- U.S. regulations prevented the export of encryption technologies with strong encryption, defined as encryption using keys of 56 bits or larger.
  - 1992, and was gradually eased until 2000



Source: Forbes,
"5 Essential Privacy Tools For The Next Crypto War"

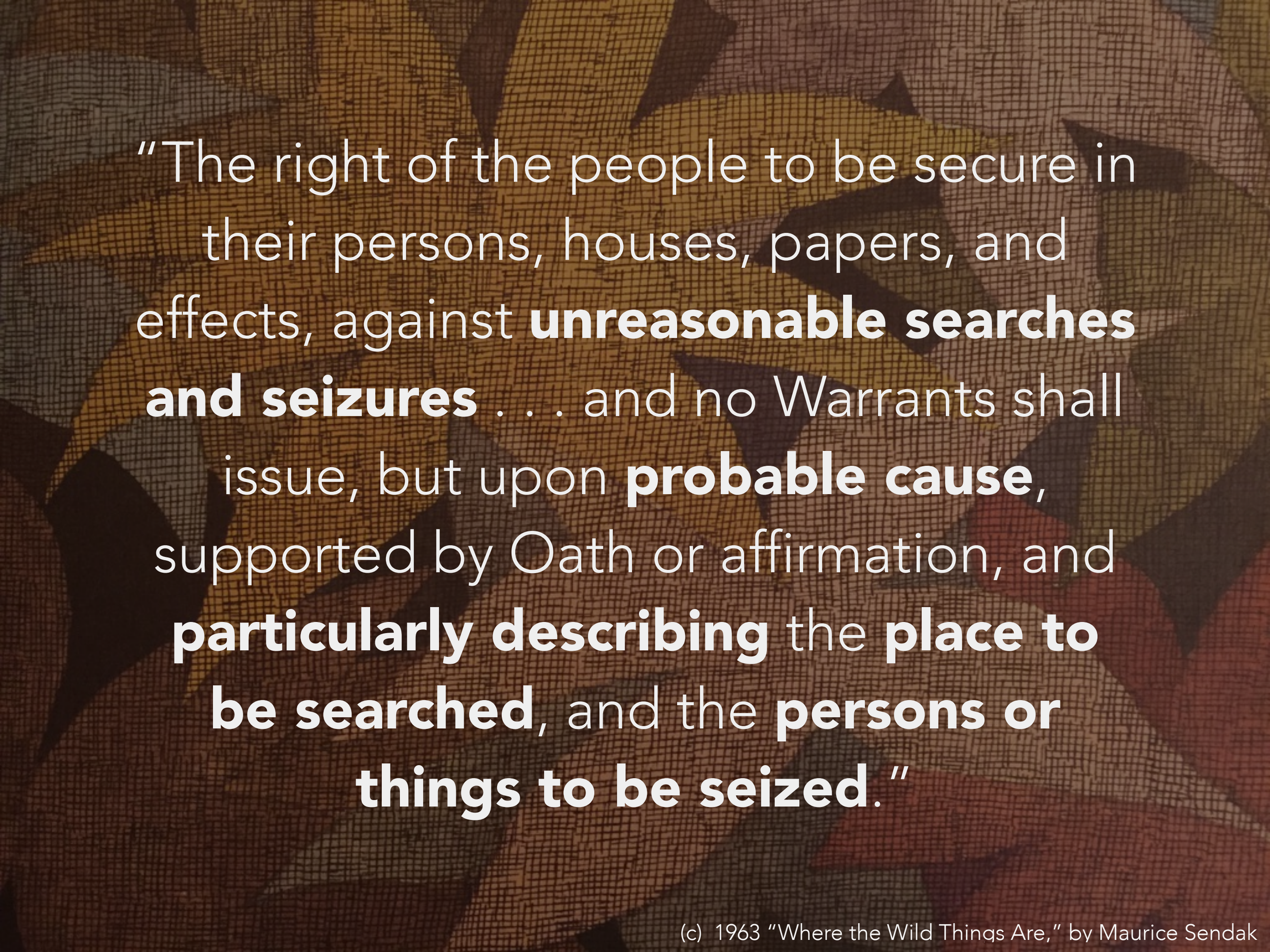
CRYPTO PROTECTED BY 1ST AMENDMENT

- "Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is **protected by the First Amendment.**" Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000)

- "**We conclude that encryption software, in its source code . . . must be viewed as expressive for First Amendment purposes**, and thus is entitled to the protections of [the First Amendment]." Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.) reh'g granted, opinion withdrawn, 192 F.3d 1308 (9th Cir. 1999)

- "[B]ecause the regulations apply to encryption source code, it necessarily follows that the regulations **burden a particular form of expression directly.**" Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1142 (9th Cir.),

4TH AMENDMENT


"The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable searches and seizures** . . . and no Warrants shall issue, but upon **probable cause**, supported by Oath or affirmation, and **particularly describing** the **place to be searched**, and the **persons or things to be seized**."
(c) 1963 "Where the Wild Things Are," by Maurice Sendak

4TH AMENDMENT IS ABOUT

LAWFUL ACCESS

NO WARRANT NEEDED

- Not a search
    - Informants or coconspirators who wear a wire
    - False friends – those lovely friends who take what you tell them and tell the police, not under the direction of the police.
    - Private actors
        - Undercover officers
        - **Phone company, Internet, or other company (3rd Party Doctrine)**
        - Trash: No reasonable expectation of privacy in garbage because assumption of risk for bums, animals, kids, and other rummaging.
        - Consent
- Plain view
- Border Search

Probable cause to believe

- A crime has been or is being committed AND
- That the items subject to seizure by virtue of their connect to the crime.

(c) 1963 "Where the Wild Things Are," by Maurice Sendak

PROBABLE CAUSE

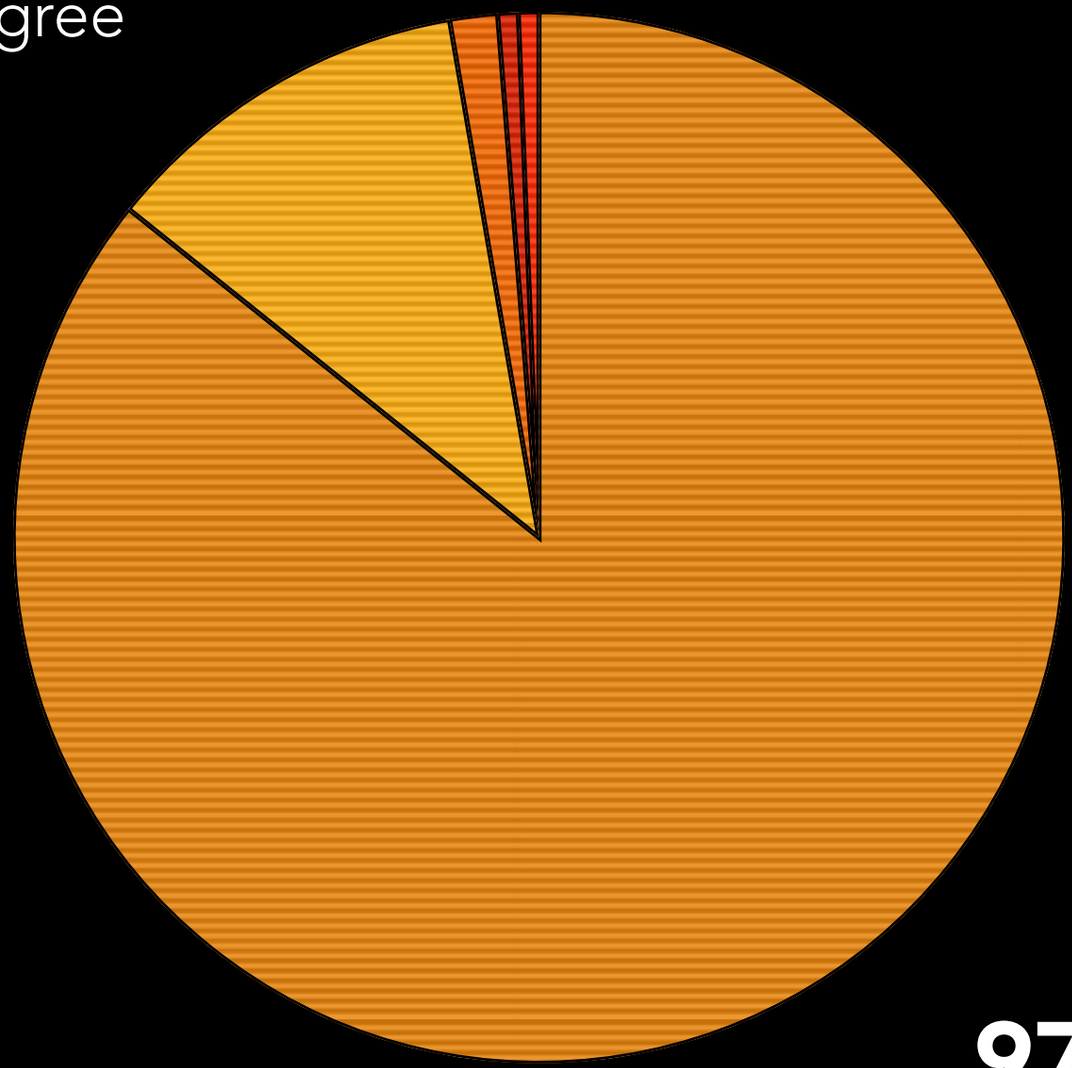
- Does the use of encryption play a role in the probable cause or reasonable suspicion analysis?

Four of the detainees have been released, but seven have been jailed pending trial. The reasons given by the judge for their continued detention include the posession of certain books, "the production of publications and forms of communication", and the fact that the defendants "used emails with extreme security measures, such as the RISE UP server" [2].

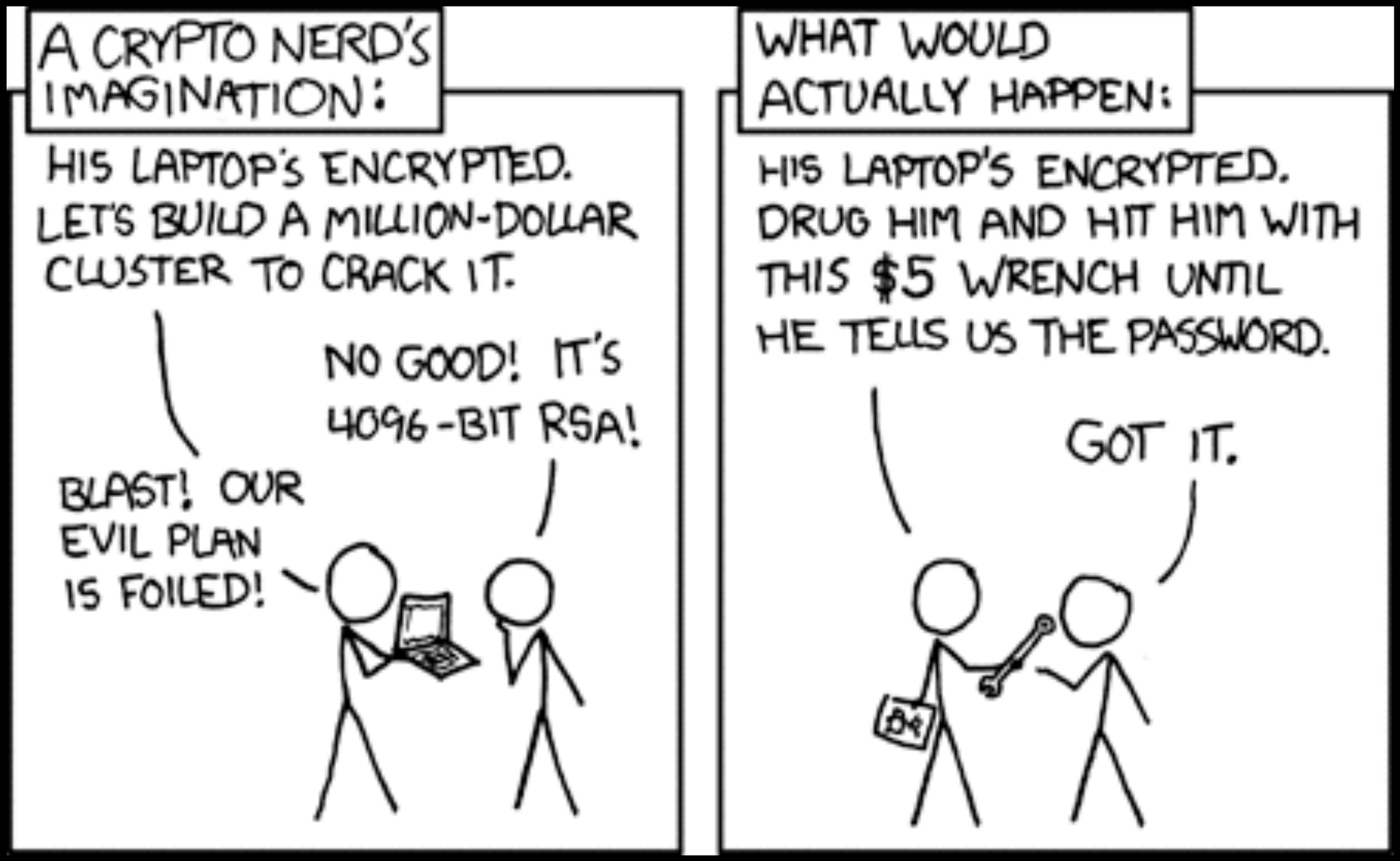
No major caselaw. Possible area to watch

ENCRYPTION IS ONLY FOR THOSE WHO HAVE SOMETHING TO HIDE.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree



97.27% Disagree



http://xkcd.com/538/

5TH AMENDMENT

"[N]o person . . . shall be **compelled** in any criminal case to be a witness against himself [or herself.]"

5TH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION

AKA:

- "I plead the 5th."
- "On counsel's advice, I invoke my right under the Fifth Amendment not to answer, on the grounds I may incriminate myself."

BUT:

- What about my "right to remain silent"?(Miranda)

(c) the Simpsons, Season 2, Ep. 31

But these phrases are not magic! Invoking the privilege does not mean **automatic and absolute** protection.

PROTECTION

- Protects and individual (not a corporation) "from compulsory incrimination through his own testimony or personal records."
- Can be asserted any time.
- "[C]an be asserted in any proceeding, civil or criminal, administrative or judicial, investigatory or adjudicatory," *Kastigar v. United States*, 406 U.S. 441, 445 (1972)

SIMPLY, FOR THE PRIVILEGE TO APPLY THERE **MUST BE**:

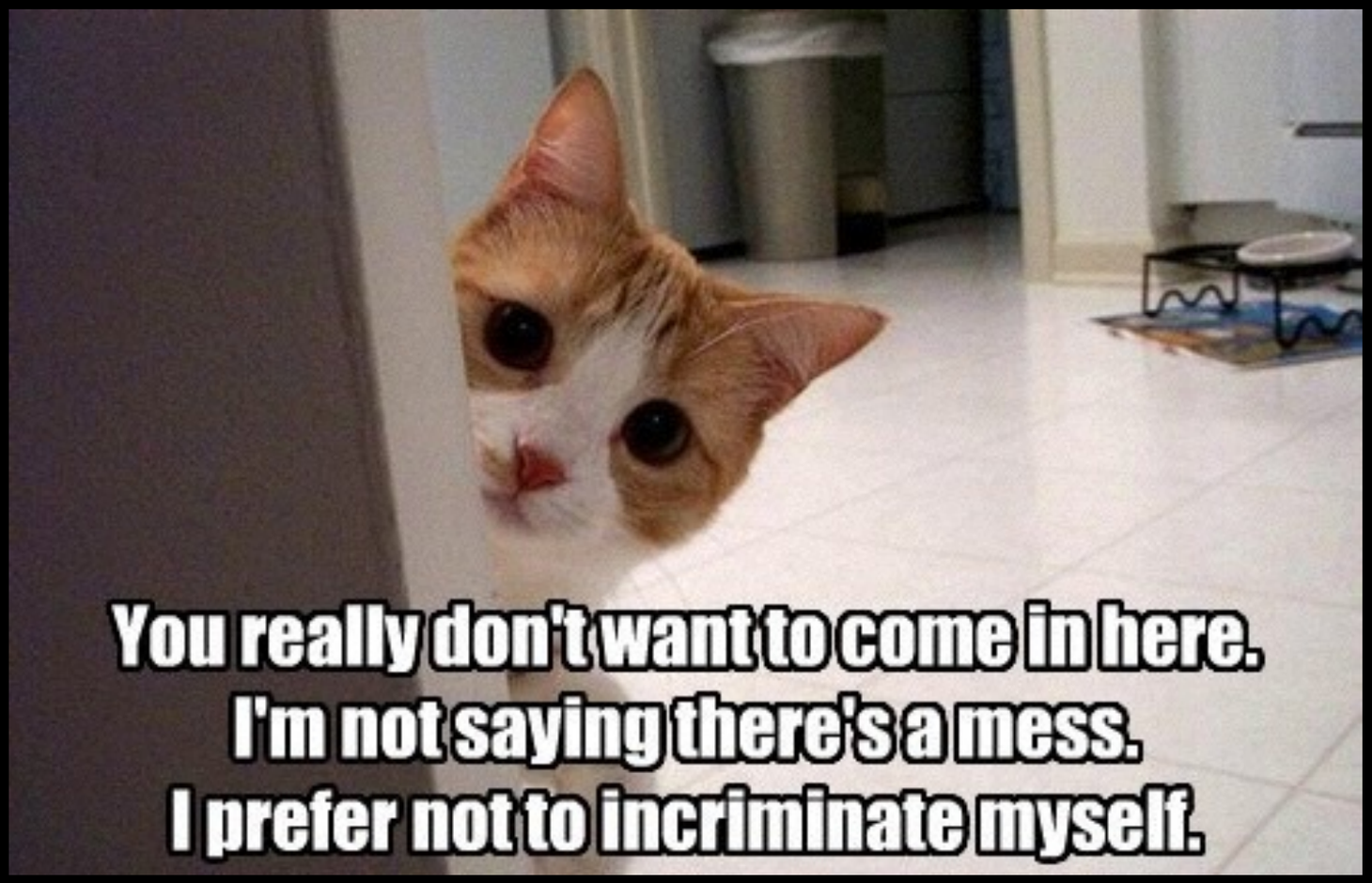
1. COMPULSION
2. SELF-INCRIMINATION
3. TESTIMONIAL COMMUNICATION OR ACT

C O M P U L S I O N

By government

- Court Order
- Grand Jury

SELF-INCRIMINATING



- Answer given:
  - supports a conviction, or
  - provides a link in the chain of evidence that **might** lead to incriminating evidence
  - do not have to be guilty to invoke privilege.

“The privilege protects the innocent as well as the guilty.”

“[O]ne of the Fifth Amendment's basic functions is to protect **innocent persons** who might otherwise be **ensnared by ambiguous circumstances**.”

OHIO V. REINER, 532 U.S. 17 (2001)

BASICALLY...

A self-incriminating statement can be just a statement that tends to **increase** the danger that the person making the statement will be **accused, charged, or prosecuted**

TESTIMONIAL = REVEALS THE CONTENTS OF YOUR MIND

- **Oral Statements:** reveal something that only exists within the individual's mind

- **Actions:** a bit more difficult…

(c) Touchstone Pictures, "Signs"

"[D]efendant's statement as to the password was testimonial in nature."

U.S. V. ROGOZIN, NO. 09–CR–379 (S)(M), 2010 WL 4628520 (W.D.N.Y NOV. 16, 2010)

TESTIMONIAL ACT

- Providing blood samples, finger prints, voice samples, and writing samples are **NON-testimonial** and thus NOT protected.

- When does an act reveal the contents of your mind?
  - Usually arises in **document production**.

- Government can compel if *merely* a physical act

WHAT DOES TURNING

OVER DOCUMENTS

REVEAL?

ACT-OF-PRODUCTION DOCTRINE

- Producing documents has communicative aspects
- **Implicitly communicates** statements of fact.
- Individual admits by producing documents:

1. documents exist
2. they are authentic
3. they are in the individual's possession or control.

PROBLEM:

ACT-OF-PRODUCTION DOCTRINE

IS INSANELY **FACT SPECIFIC**

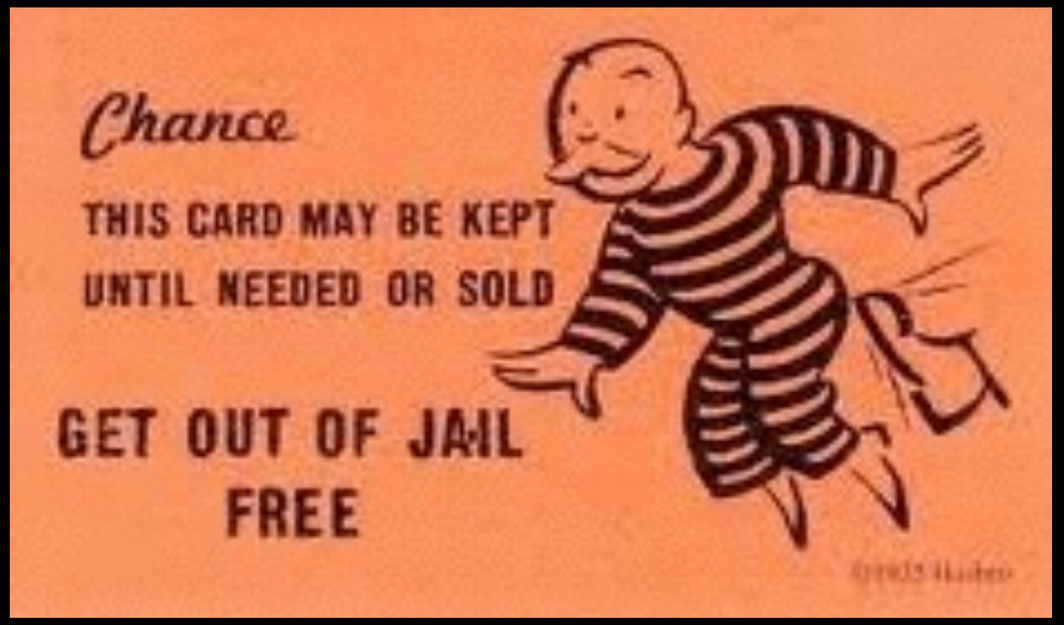
IF GOVERNMENT:

- can show with "reasonable particularity" that when it sought to compel production that they already knew the materials sought existed (forgone conclusion);
- gathers the information another way; or
- grants immunity

NO TESTIMONIAL ACT

OBTAINING INFORMATION ANOTHER WAY

- Other evidence
- Bypassing security
- Backdoor, brute force etc.



IMMUNITY

- Then no longer incriminating.

FORGONE CONCLUSION/ REASONABLE PARTICULARITY

- Demonstrated by testimony by third party that individual **possesses the documents**

- Individual being subpoenaed acknowledged that the **documents existed** and were **in his or her possession**

- Have evidence that indicates the subpoenaed **documents already exist** and **are in the individuals possession**

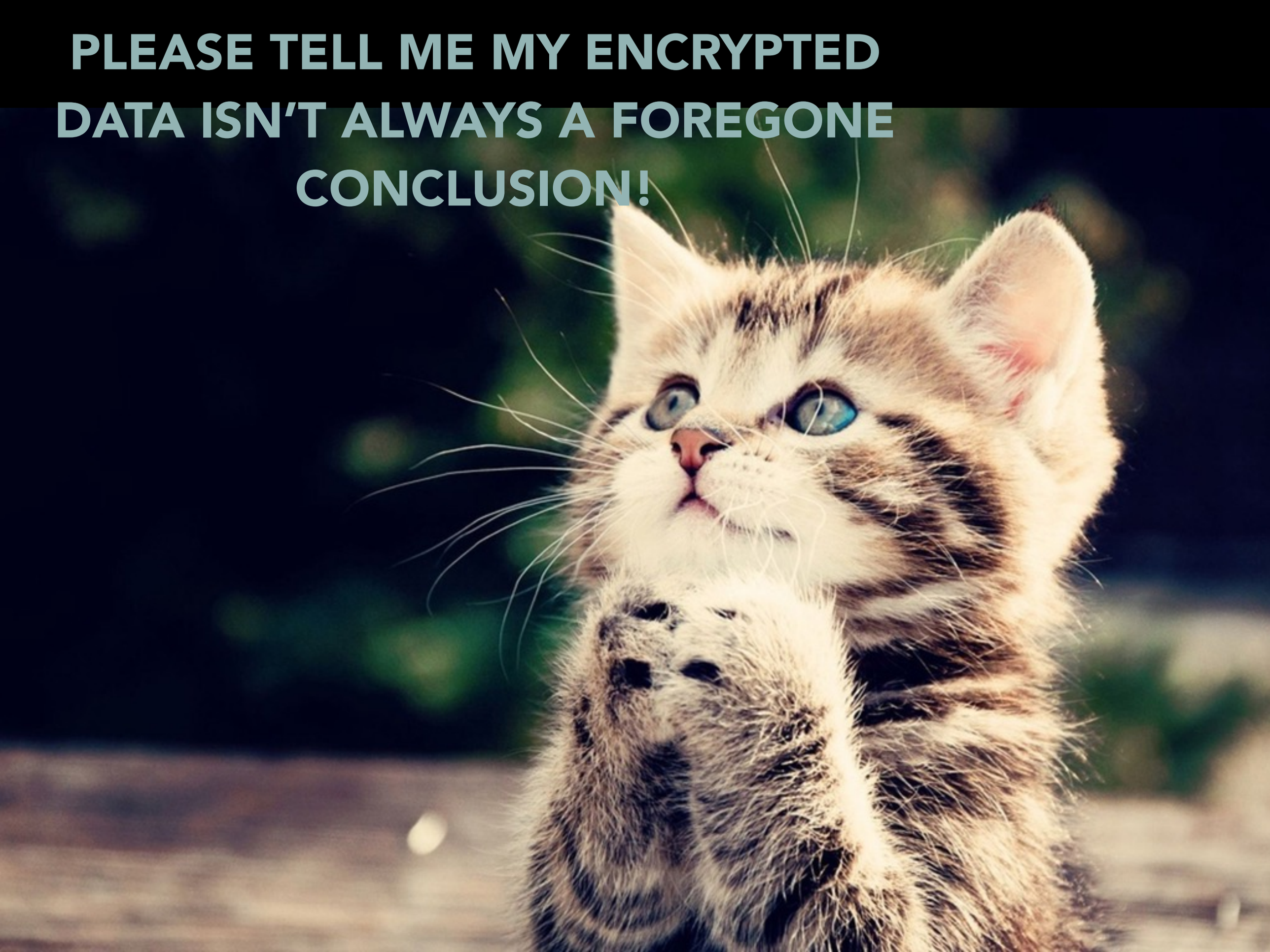
- documents are the type that exist in the course of doing business (narrowed slightly).

ACT-OF-PRODUCTION DOCTRINE

- Producing documents has communicative aspects
- Implicitly communicates statements of fact.
- Individual admits by producing documents:

1. **documents exist**
2. **they are authentic**
3. **they are in the individual's possession or control.**

PLEASE TELL ME MY ENCRYPTED DATA ISN'T ALWAYS A FOREGONE CONCLUSION!



SUDO GIVE ME YOUR PASSPHRASE

- Only a few courts have examined whether or not individual's Fifth Amendment right against self-incrimination completely protects forced disclosure of a password, encryption key, or decrypted version of the documents.

- Where the courts differ: **FOREGONE CONCLUSION**

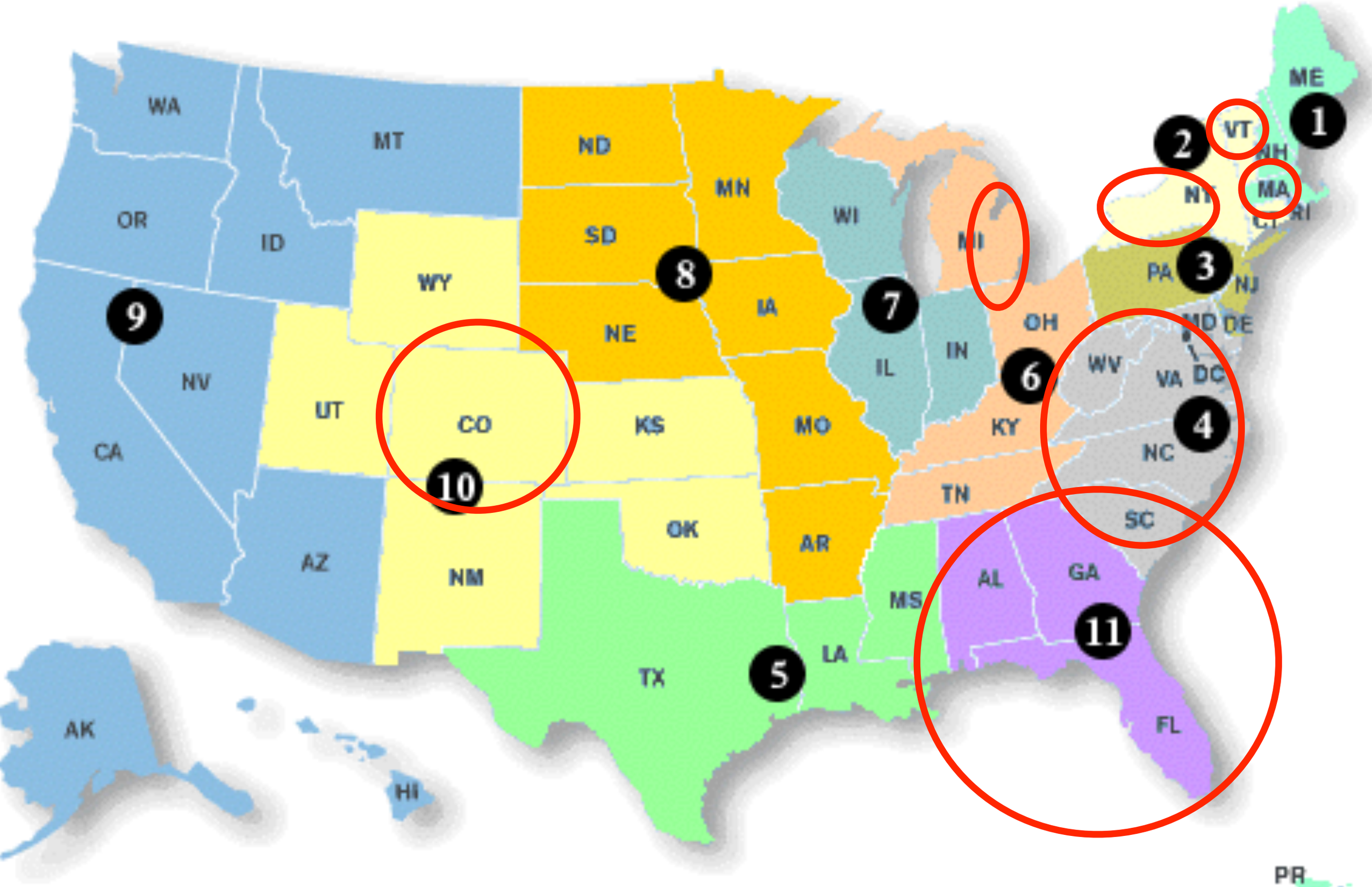
Whether or not the 5th Amendment privilege against self-incrimination applies in forced decryption cases depends on if the evidence revealed through turning over a password or decrypted documents is a **forgone conclusion.**

Any self-incriminating testimony that he may have provided by revealing the password was already a "foregone conclusion" because the Government independently proved that Gavegnano was the sole user and possessor of the computer.

U.S. V. GAVEGNANO, 305 FED.APPX. 954, 956 (4TH CIR. 2009)

THE CASES:

- *Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014)
- *In re The Decryption of a Seized Data Storage System (Feldman)*, 13-M-449 (E.D. Wis. 2013)
- *In re Grand Jury Subpoena Duces Tecum (Doe)*, 670 F. 3d 1335 (11th Cir. 2012)
- *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012)
- United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010)
- U.S. v. Rogozin, No. 09–CR–379 (S)(M), 2010 WL 4628520 (W.D.N.Y Nov. 16, 2010)
- *U.S. v. Gavegano,* 305 Fed.Appx. 954 (4th Cir. 2009)
- *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009)


WA
MT
ND
MN
OR
ID
SD
WI
MI
WY
NY
VT
NH
ME
MA
RI
CT
NJ
PA
NE
IA
IL
IN
OH
MD
DE
WV
VA
DC
NV
UT
CO
KS
MO
KY
NC
CA
AZ
NM
OK
AR
TN
SC
MS
AL
GA
TX
LA
FL
AK
HI
PR
1
2
3
4
5
6
7
8
9
10
11

ALL WRITS ACT

GIZMODO

+ FOLLOW

Feds Use 18th Century Law to Force Apple to Unlock Encrypted Phones

Adam Clark Estes

Filed to: PRIVACY 12/01/14 12:23pm

36,239 3 ★

WELL...NO.

NOTHING NEW

- Gives federal courts authority to issue writs (court orders) that are "**necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.”**

- Requires 3rd parties to assist in execution of prior court order

- Cannot use to bypass Constitutional rights
- Cannot use if "unreasonably burdensome"

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge Robert E. Blackburn

Criminal Case No. 10-cr-00509-REB-02

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. RAMONA CAMELIA FRICOSU,
a/k/a Ramona Smith,

Defendant.

ORDER GRANTING APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT FRICOSU TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS

Blackburn, J.

The matters before me are (1) the government's **Application Under the All Writs Act Requiring Defendant Fricosu To Assist in the Execution of Previously Issued Search Warrants** [#111][1] filed May 6, 2011; and (2) **Ms. Fricosu's Motion for Discovery – Seized Hard Drive** [#101] filed April 27, 2011. I held hearings on these motions on November 1, 2011, and January 3, 2012, at which I received evidence and argument.

In fashioning my ruling, I have considered all relevant adjudicative facts in the file and record of this case. I have considered the evidence educed at the hearings on

BACKDOORS OR THE GOLDEN KEY

Oh so golden...

LEGISLATION FOR MANDATED BACKDOOR

- Constitutional
- All Writs Act DOES NOT give this authority
    - "unreasonably burdensome"
    - UNLESS backdoor already exists
- Currently, unlikely to happen.

House Representatives Darrell Issa, Zoe Lofgren, Senator Ron Wyden say **"zero chance"** they will pass a bill forcing companies to install backdoor access in device encryption for federal investigators.

INTELLIGENCE

5.	(TS//SI) The fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information	TOP SECRET// COMINT *at a minimum*

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

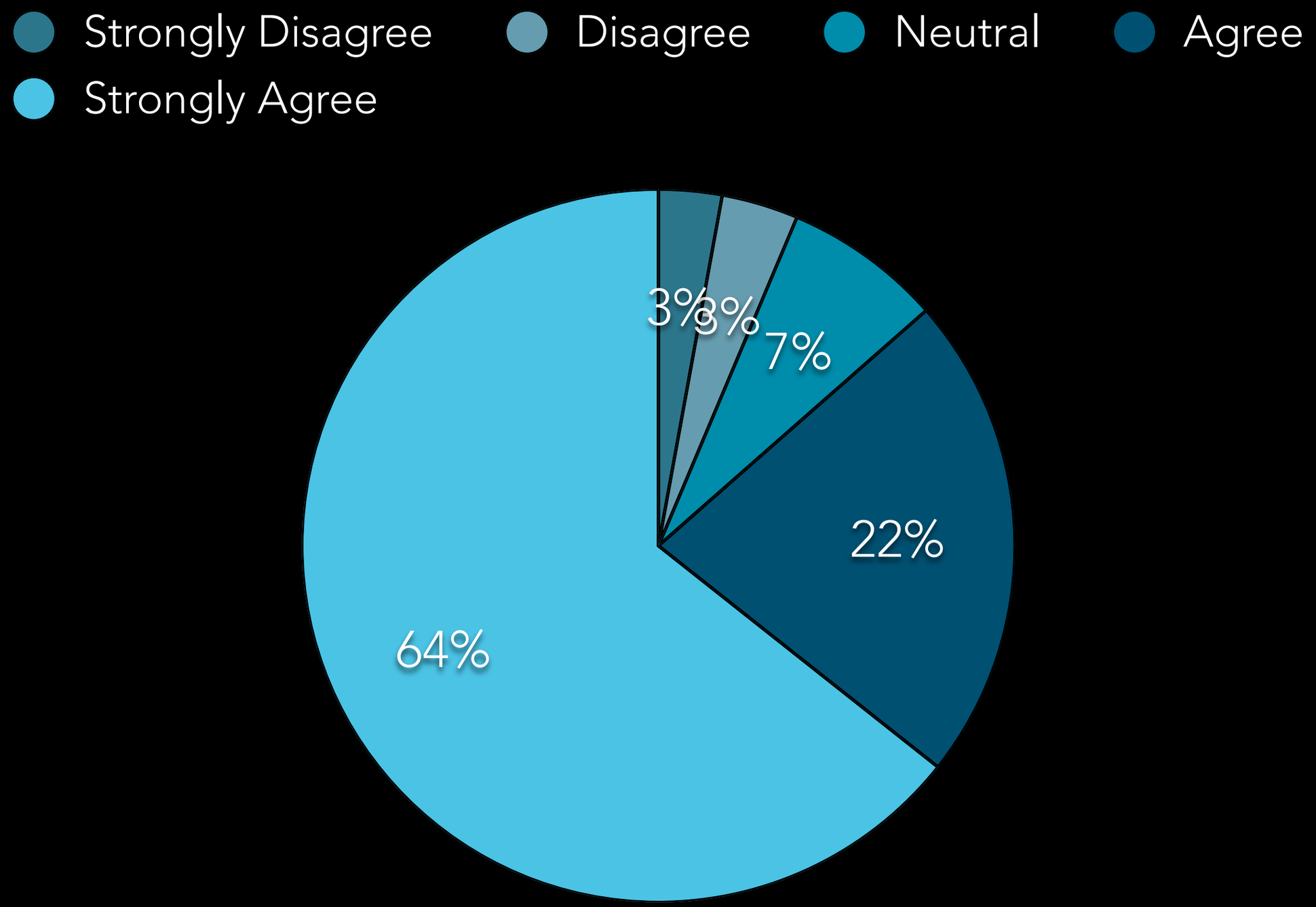
Happy Dance!!

exploitation is unrealistic

- DECRYPTS, DECRYPTS, DECRYPTS!!!!!!

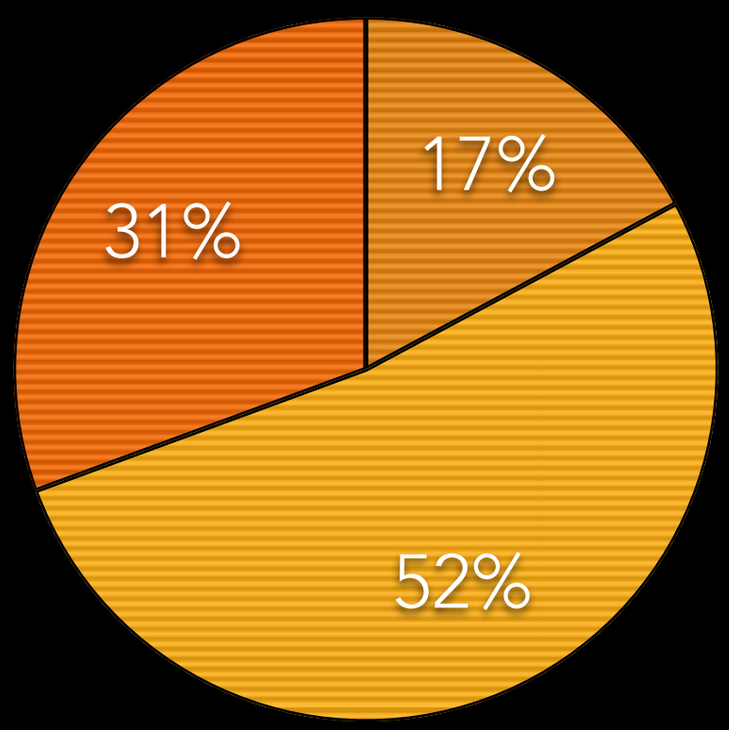
THE USERS AND ENCRYPTION: SOME RESEARCH

ENCRYPTION SHOULD BE TURNED ON BY DEFAULT



477 PARTICIPANTS

- Biggest Split:
  - Question 12: The government **should** be able to force an individual to decrypt personal information under the proper legal measures (a warrant or court order).



52.2% - Disagree
31.61% - Agree
17.19% - Neutral

AGREE VS. DISAGREE

- Agree = more casual about privacy rights/ protections
- Almost all believe in fundamental right to privacy — but not necessarily with respect to privacy rights from the government.
- Disagree = More likely to use disk encryption or password protect phone
- Both disagree that encryption is ONLY for those who have something to hide.

GOING

FORWARD

UPSET BALANCE

If the police have lawful access, but no technological access. Should technological access barriers always defeat legal access barriers?

WHAT'S NEXT?

MORE ENCRYPTION!
- ESTABLISHED 5TH AMENDMENT CASELAW
- BIOMETRIC VS. PASSPHRASE

LEGAL DEBATE ABOUT BALANCE
- CONTINUED TO BE WORKED OUT IN COURTS
- WILL FOREGONE CONCLUSION BE ENOUGH?

PROBABLE CAUSE
- LESS LIKELY TO FACTOR INTO ANALYSIS AS IT BECOMES INCREDIBLY PREVALENT

THANK YOU

- The Shmoo Group & ShmooCon
- The University of Illinois Urbana-Champaign
- Masooda Bashir & Boyi Guo

Questions?
@wbm312